Youthful Indiscretions

Should Colleges Protect Social Network Users from Themselves and Others?

DANA L. FLEMING

Counting members in the hundreds of millions, online social networking communities such as MySpace and Facebook may prove nearly as transformative as the 1876 invention of the telephone. Creating a MySpace or Facebook profile is free and making online "friends" is easy—if you're under 30. But students' online identities and friendships come at a price, as job recruiters, school administrators, law enforcement officers and sexual predators sign on and start searching.

MySpace is routinely ranked among the top three most popular websites in America. The site was founded in 2003 by Tom Anderson, a graduate student at UCLA. Two years later, Rupert Murdoch's News Corp. purchased MySpace for a reported $327 million. Beyond its financial success, MySpace boasts an international audience with more users than any other networking site in the world.

In New England, however, Facebook is a local favorite among college students and recent graduates, perhaps because it was founded in the region, by then Harvard sophomore Mark Zuckerberg. The first month the site went "live" in 2004, half of Harvard's undergraduates signed up. Its popularity spread to other Boston-area campuses including MIT, Boston University and Boston College. By December 2004, the number of registered Facebook users surpassed one million. Facebook began by catering to undergraduates and for many years restricted membership by requiring all users to have a ".edu" email account. In recent years, Facebook has opened its site to a wider audience in order to serve the growing demand for online social networking. Yet, Facebook remains the most popular site among New England college students.

Other sites such as Friendster, LiveJournal and YouTube offer additional means for users to "broadcast" their innermost thoughts and secrets across the World Wide Web. To join, a user needs only an email address and a willingness to share his or her "profile" with other users. Profiles usually include pictures and personal descriptions, music and video clips, plus information about the user's relationship status, school

continued on next page

affiliations, interests and hometown. "Friending" someone (yes, it's a verb now) is as easy as searching for a name and clicking on it. This automatically sends a "friend request" to the other user, which that user can then accept, simply by clicking on the request. Perhaps not surprisingly, it is commonplace for users to have hundreds, even thousands of friends. Thirty percent of students report accepting "friend" requests from total strangers.

Joining or forming groups on these networks is easy too. With just a few clicks, users can join "Drunks United," "Sexy and Single on MySpace," or "My B.A.C. is Higher Than Your GPA." All of these groups have memberships in the tens of thousands. While privacy settings allow users to restrict who may view their profiles and group affiliations, such settings are rarely enabled by the user. Even when access is restricted to a user's so-called "friends," when students have hundreds or even thousands of "friends," anonymity can be hard to come by.

The explosion in online social networking sites and attendant loss of anonymity carries a cost. One University of Chicago student ruined his chances at a summer internship when an executive from the company viewed his Facebook profile, only to discover that his interests included "smoking blunts" (cigars stuffed with marijuana), shooting people, and obsessive sex. A chemical engineering major sabotaged his career in a similar manner by confessing in his online bio that he liked to "blow things up."

Recruiters are not the only ones checking up on students' profiles. In May 2005, two swimmers at Louisiana State University lost athletic scholarships for making disparaging comments about their coach on Facebook. In October 2005, a student at Boston's Fisher College was reportedly expelled for defaming a college police officer on Facebook. In an ongoing dispute at Millersville University in Pennsylvania, a young woman was denied her teaching degree after a fellow student brought one of her MySpace photos to the attention of school administrators. The photo, which has spurred a lawsuit, features the young woman wearing a pirate hat, drinking from an opaque plastic cup. The photo is suggestively captioned "Drunken Pirate."

A private Christian university in Virginia got creative when it found out that one of its law students posted an unflattering video of the school's founder, Pat Robertson, on Facebook and YouTube. (In the video, Pat Robertson appears to scratch his face with his middle finger.) The university has demanded that the law student publicly apologize for the posting or submit a legal brief defending it as satire protected under the First Amendment. Reports indicate that the student has chosen the latter punishment.

The dangers of online social networking transcend disciplinary actions and reputational harm. A 17-year-old Rhode Island girl was reportedly drugged and raped by three men she befriended on MySpace. Detectives in Colorado recently used MySpace to identify six men involved in the brutal rape and robbery of one of their online "friends." And the parents of a 13-year-old girl from Texas blame MySpace for their daughter's sexual assault and tried unsuccessfully to sue the company for negligence. The girl, "Julie Doe," lied about her age on her MySpace profile, then agreed to meet one of her "friends" in a restaurant parking lot where her friend, a 19-year-old male, sexually assaulted her. A U.S. District Court Judge dismissed the suit, stating: "If anyone had a duty to protect Julie Doe, it was her parents, not MySpace."

Parents groups, attorneys general and legislators are grappling with how to protect young users from other users and, still more challenging, how to protect young users from themselves. Forty-five attorneys general are pushing MySpace to adopt more parental controls and an age-verification system. For example, Connecticut Attorney General Richard Blumenthal wants to see MySpace raise its minimum age limit from 14 to 16. Several bills in Congress have included provisions barring schools and libraries that receive federal funding from allowing minors to access networking sites like MySpace and Facebook.

Like lawmakers, college administrators have not yet determined how to handle the unique issues posed by the public display of their students' indiscretions. While some are starting to develop very thoughtful policies about these sites, many still wonder what all the fuss is about. Some schools use material from MySpace and Facebook in their judiciary proceedings while others turn a blind eye to the site. Some address the risks associated with these sites during freshman orientation, while others let students proceed at their own risk.

The office of student affairs at the University of Maine warns that while "the administrators are not monitoring Facebook," they may act on any violations of law or University policy if it is brought to their attention. As the school candidly puts it: "Just because you don't want them [the administrators] to look at your page doesn't mean they can't or won't." Norwich University offers this reminder to its students: "As an institution of higher learning, Norwich University recognizes the importance of free speech and the use of information technology in the pursuit of educational goals. Nonetheless … we are all expected to behave—on campus, in public and online—in a manner consistent with the University's Honor Code and Guiding Values."

The Norwich policy, like many others across the country, is followed by a series of practical tips for online networkers, such as: "Don't post anything you wouldn't be comfortable with your grandmother seeing." Good advice, to be sure, but even a cursory perusal of these sites suggests that many students are not listening.

continued on next page

There is no practical way for colleges to monitor the content of these sites, as students' profiles and postings are changing *constantly*. It would take a full-time staff working around the clock to scratch the surface of a single network. An aggressive monitoring approach can also backfire. When students find out that a network is being monitored by administrators, they frequently change networks, password-protect their profile or group or post misleading information to confuse and frustrate administrators, (e.g., one student advertised a frat party at a specific dorm room, only to leave a "gotcha" note for campus police).

While a blanket monitoring approach is infeasible, if not counter-productive, a targeted review of online social networking sites can be a good thing. For example, when a student exhibits signs of distress, a review of his or her online profile or blog may be appropriate. A review of a student's profile may also be appropriate where that student is involved in a disciplinary proceeding. Courts treat people's online postings as evidence in criminal proceedings, and college and university lawyers routinely check students' online profiles. It stands to reason then, that schools are free to use content from these sites in their own judiciary proceedings. Colleges that wish to create a policy specially tailored to online social networking policies should review Cornell's University's "Thoughts on Facebook," which cautions students about the personal risks and legal ramifications of online social networking, while at the same time acknowledging the benefits and popular appeal of such sites.

In this era of aggressive data-mining and total information access, students' privacy is in peril. Advertisers are particularly interested in students' personal information, as they try to tailor ads to individual users. For example, a restaurant may create an online advertisement based not only on the student's geographic location, but also by noting that one of their "friends" is a regular customer. This type of targeted advertising helps to explain the financial success of sites like MySpace and Facebook where online advertisers can pay as much for online advertising space as they do for commercial slots on primetime TV.

Under the Family Educational Rights and Privacy Act (FERPA), colleges have a responsibility not to divulge students' personal information, sell their names, phone numbers and email addresses to advertisers or otherwise violate their privacy rights. But when students post their most intimate secrets online, how can schools protect students' privacy?

Though many students believe that the information they post online is "private," it's not—and the simplest way to address the liabilities posed by these sites is to treat them like any other university activity, subject to the school's code of conduct and applicable state and federal laws.

Dana L. Fleming *is a Boston-area attorney specializing in higher education law.*
Email: dfleming@seyfarth.com.